CLAIMS

Therefore, having thus described the invention, at least the following is claimed:

1. A method for scrambling a digital data stream for use in a non-self synchronizing scrambling (NS3) communication system, said digital data stream comprising a series of bits and having a bit transmission rate, the method comprising the steps of:

generating a pseudo-noise sequence (PNS), said PNS having a timing reference distinct from said series of bits and said bit transmission rate of said digital data stream; and

modifying said digital data stream based on said PNS to produce a scrambled digital data stream, wherein said scrambled digital data stream is capable of being descrambled by performing the inverse of said modifying step.

2. The method of claim 1, wherein said generating step further comprises deriving a set of symbol indices from said digital data stream; and wherein said modifying step further comprises combining said symbol indices and said PNS to produce a symbol-wise scrambled digital data stream.

3. The method of claim 1, wherein said generating step further comprises generating said PNS with an encryption algorithm.

4. The method of claim 2, wherein said modifying step further comprises modulo-2 adding of said symbol indices and said PNS.

5. The method of claim 2, wherein said modifying step further comprises arithmetic adding of said symbol indices and said PNS.

6. The method of claim 2, wherein said common timing reference is a whole or fractional multiple of the time interval between each symbol in said set of symbol indices.

7. A method for using non-self synchronizing scrambling (NS3) in a communication system, comprising the steps of:

scrambling a digital data stream, said data stream comprising a series of bits and having a transmission rate;

descrambling said scrambled digital data stream;

establishing synchronization between said scrambling step and said descrambling step; and

maintaining synchronization between said scrambling step and said descrambling step by means of a common timing reference, said common timing reference being distinct from said series of bits and said bit transmission rate of said digital data stream.

8. The method of claim 7, wherein said common timing reference is a whole or fractional multiple of the time interval between each symbol in said set of symbol indices.

9. The method of claim 7, wherein said scrambling step is performed in a first communication device located at an ingress point to a communication medium and said descrambling step is performed in a second communication device located at an egress point to the communication medium.

10 The method of claim 7, wherein said establishing step comprises a training sequence.

11. The method of claim 7, wherein said scrambling step further comprises:

deriving a set of symbol indices from said digital data stream;

generating a first pseudo-noise sequence (PNS); and

combining said symbol indices and said first PNS to produce a symbol-wise scrambled digital data stream.

12. The method of claim 11, wherein said combining step comprises modulo-2 adding of said symbol indices and said first PNS.

13. The method of claim 11, wherein said combining step comprises arithmetic adding of said symbol indices and said first PNS.

14. The method of claim 11, wherein said descrambling step further comprises:

generating a second PNS, said second PNS being identical to said first PNS;

combining said second PNS with said symbol-wise scrambled digital data stream to produce a symbol-wise descrambled digital data stream; and

deriving a conventional bit-wise descrambled digital data stream from said symbol-wise descrambled digital data stream.

15. The method of claim 14, wherein said combining step comprises modulo-2 adding of said second PNS with said symbol-wise scrambled digital data stream.

16. The method of claim 14, wherein said combining step comprises subtracting said second PNS from said symbol-wise scrambled digital data stream.

17. The method of claim 7, further comprising the steps of:

detecting loss of synchronization; and

reestablishing synchronization.

18. The method of claim 17, wherein said reestablishing step comprises a retraining sequence.

19. A communication device for scrambling a digital data stream for use in a non-self synchronizing scrambling (NS3) communication system, said digital data stream comprisng a series of bits and having a bit transmission rate, the communication device comprising:

means for generating a pseudo-noise sequence (PNS), said PNS having a timing reference distinct from said series of bits and said bit transmission rate of said digital data stream; and

means for modifying said digital data stream based on said PNS to produce a scrambled digital data stream, wherein said scrambled digital data stream is capable of being descrambled by a second modifying means that is the inverse of said modifying means.

20. The communication device of claim 19, further comprising:

means for transmitting said scrambled digital data stream.

21. The communication device of claim 19, wherein said generating means is an encryption device.

22. The communication device of claim 19, wherein said modifying means is a modulo-2 adder.

23. The communication device of claim 19, wherein said modifying means is an arithmetic adder.

24. The communication device of claim 19, wherein said generating means further comprises means for deriving a set of symbol indices from said digital data stream; and wherein said modifying means further comprises combining said symbol indices and said PNS to produce a symbol-wise scrambled digital data stream.

25. The communication device of claim 24, wherein said timing reference is a whole or fractional multiple of the time interval between each symbol in said set of symbol indices.

26. A non-self synchronizing scrambling (NS3) communication system, comprising:

a first communication device having means for scrambling and transmitting a first digital data stream, said data stream comprising a series of bits and having a transmission rate;

a second communication device having means for receiving and descrambling said first scrambled digital data stream;

means for establishing synchronization between said first communication device and said second communication device; and

means for maintaining a common timing reference for said first communication device and said second communication device, said common timing reference being distinct from the series of bits and the bit transmission rate of said first digital data stream.

27. The system of claim 26, wherein said common timing reference is a whole or fractional multiple of the time interval between each symbol in said set of symbol indices.

28. The system of claim 26, wherein said means for establishing synchronization is a training sequence.

29. The system of claim 26, wherein said scrambling means further comprises:

means for converting said first digital data stream from bits to symbols;

means for generating a first PNS; and

means for combining said symbols and said first PNS to produce a first symbol-wise scrambled digital data stream.

30. The system of claim 29 wherein said converting means is a bit-to-symbol converter.

31. The system of claim 29, wherein said combining means is a modulo-2 adder.

32. The system of claim 29, wherein said combining means is an arithmetic adder.

33. The system of claim 29, wherein said descrambling means further comprises:

means for generating a second PNS;

means for combining said second PNS and said first symbol-wise scrambled digital data stream to produce a first symbol-wise descrambled digital data stream; and

means for converting said first symbol-wise descrambled digital data stream from symbols to bits.

34. The system of claim 33 wherein said converting means is a symbol-to-bit converter.

35. The system of claim 33, wherein said combining means is a modulo-2 adder.

36. The system of claim 33, wherein said combining means is an arithmetic subtractor.

37. The system of claim 33, wherein synchronization is established between said scrambling means and said descrambling means by initializing said first generating means and said second generating means with the same predetermined value.

38. The system of claim 33, wherein said second communication device further comprises means for scrambling and transmitting a second digital data stream and wherein said first communication device further comprises means for receiving and descrambling said second scrambled digital data stream.

39. The system of claim 38, wherein said first communication device and said second communication device operate bidirectionally.

40. The system of claim 38, wherein said scrambling means in said second communication device further comprises:

means for converting said second digital data stream from bits to symbols; and

means for combining said symbols and said second PNS to produce a second symbol-wise scrambled digital data stream;

and wherein said descrambling means in said first communication device further comprises:

means for combining said first PNS and said second symbol-wise scrambled digital data stream to produce a second symbol-wise descrambled digital data stream; and

means for converting said second symbol-wise descrambled digital data stream from symbols to bits.

41. The system of claim 39, wherein said first communication device is an Digital Subscriber Line Transceiver Unit – Central Office (DTU-C) and said second communication device is an Digital Subscriber Line Transceiver Unit – Remote (DTU-R).

42. The system of claim 40, wherein said scrambling means in said second communication device begins scrambling the second digital data stream substantially simultaneously with completion of descrambling of the first scrambled digital data steam by said descrambling means in said second communication device.

43. The system of claim 41, further comprising a plurality of additional DTU-Rs, said plurality of additional DTU-Rs having the same capabilities as said second communication device.

44. The system of claim 42, wherein the substantially simultaneous completion of descrambling of said first digital data stream and the beginning of scrambling of said second digital data stream comprises using the state of the second PNS generator at the time of completion of said descrambling as the initial state of said second PNS generator for scrambling said second digital data stream.

45. The system of claim 42, wherein said first communication device further comprises a FIFO register to store previous states of said first PNS generator.

46. The system of claim 42, further comprising means for delaying said second PNS, wherein said combining means combines said delayed second PNS and said symbols to produce the second symbol-wise scrambled digital data stream.